ABSTRACT OF THE DISCLOSURE

A trusted authority delegates authority to a device. This delegation of authority is effected by providing a yet-to-be completed chain of public/private cryptographic key pairs linked in a subversion-resistant manner. The chain terminates with a penultimate key pair formed by public/private data, and a link towards an end key pair to be formed by an encryption/decryption key pair of an Identifier-Based Encryption, IBE, scheme. The private data is securely stored in the device for access only by an authorized key-generation process that forms the link to the end key pair and is arranged to provide the IBE decryption key generated using the private data and encryption key. This key generation/provision is normally only effected if at least one condition, for example specified in the encryption key, is satisfied. Such a condition may be one tested against data provided by the trusted authority and stored in the device.